AIMS Mathematics, 9(3): 5722–5745.
DOI: 10.3934/math.2024278
Received: 20 August 2023
Revised: 13 January 2024
Accepted: 16 January 2024
Published: 30 January 2024

http://www.aimspress.com/journal/Math

Research article

Color image encryption by piecewise function and elliptic curve over the Galois field $GF(2^n)$

Hafeez Ur Rehman[1,*], Mohammad Mazyad Hazzazi[2], Tariq Shah[1], Amer Aljaedi[3] and Zaid Bassfar[4]

[1] Department of Mathematics, Quaid-i-Azam University Islamabad, Islamabad 45320, Pakistan
[2] Department of Mathematics, College of Science, King Khalid University, Abha 61421, Saudi Arabia
[3] College of Computing and Information Technology, University of Tabuk, Tabuk 71491, Saudi Arabia
[4] Department of Information Technology, University of Tabuk, Tabuk 71491, Saudi Arabia

* **Correspondence:** Email: hrehman@math.qau.edu.pk; Tel: +923475502522.

Abstract: Elliptic curve (EC) cryptography supplies an efficient, secure, and lightweight method for executing computer cryptographic protocols. Its widespread use in various applications, including secure communications, digital signatures, and key agreement protocols, highlights its importance in modern computing. Moreover, EC-based image encryption is gaining popularity in cryptography as it offers strong protection with a relatively smaller key size than other famous cryptosystems. Inspired by this, we proposed a novel image encryption scheme that leverages ECs over a binary extension field (BEF). This approach also reduces computational workload using EC over BEF instead of large primes. Also, BEF can represent large numbers in a compact form, which is helpful in applications that require efficient data storage and transmission. Our scheme involves three main steps. Initially, we utilize points of an EC over a BEF and a piecewise function to mask the plain image. Next, to introduce a high level of confusion in the plain text, we create a substitution box (S-box) based on the EC and operation of BEF of order 256, which is then used to permute the pixels of the masked image. Finally, we generate pseudo-random numbers (PRNs) using EC coordinates and BEF characteristics to create diffusion in the image and obtain a cipher image. In addition, we accomplished computational experiments demonstrating that our proposed cryptosystem provides excellent security against linear, differential, and statistical attacks compared to existing cryptosystems.

Keywords: elliptic curve cryptography; Galois field; image encryption; S-box

Mathematics Subject Classification: 68P25, 81P94, 94A60

1. Introduction

The security of sensitive information has become a significant concern in the age of 5G networks. digital images, including agreements, paintings, medical reports, agreements, and other scanned documents, are a primary source of information requiring the highest sensitivity level. Protecting the privacy of digital images when shared between authorized parties in systems such as the cloud is of utmost importance [1]. There have been advancements in developing multiple effective encryption algorithms to protect multimedia data's security and privacy. These algorithms rely on two distinct principles: symmetric and asymmetric key algorithms. Confusion and diffusion modules are the major techniques used for symmetric algorithms [2,3]. The confusion module is usually applied after the diffusion operation has successfully severed the relationship between the ciphered data and the keys employed in image, audio and video encryption [2,4–7]. The data used in both modules are obtained from a range of numbers generated by a pseudo-random number generator (PRNG). Modern image cryptography relies heavily on well-designed PRNGs that utilize mathematical mechanisms [3,8,9]. As a result, numerous effective algorithms have been created to produce substitution boxes (S-boxes) and pseudo-random number (PRN) sequences [10–13]. In [14,15], the authors introduced a comprehensive scheme for securing images, employing a combination of chaos-based block permutation and weighted bit plane chain diffusion. Furthermore, the authors proposed a face image privacy protection scheme that relies on chaos and DNA cryptography. This dual approach addresses image security through advanced encryption techniques and the emerging need for robust privacy protection in the context of face images. In [16,17], the authors give an idea of an Image encryption algorithm based on plane-level image filtering, discrete logarithmic transform, and RNA-encoded color image encryption scheme based on a chain feedback structure. There are two types of S-boxes available: static and dynamic. Static S-boxes operate and generate outputs in fixed modes, whereas dynamic S-boxes possess multiple operating modes. Dynamic S-box algorithms are preferred because they increase computational costs for cryptanalysts. Recent studies have proposed several techniques to enhance the security of cryptographic systems. For example, Ibrahim et al. [3] introduced a method that utilizes permuted elliptic curves (ECs) to generate key-dependent dynamic S-boxes, aiming to minimize computational expenses. Alhandawi et al. [18] suggested an S-box configuration based on a modified Firefly algorithm, claiming to exhibit satisfactory cryptographic characteristics. In addition, a new algorithm utilizing a group structure was introduced in [19], which provides high nonlinearity for secure S-box generation. Furthermore, Toughi et al. [20] presented an image encryption scheme utilizing PRNG and advanced encryption standard (AES) modules, while [21] designed an image encryption method using a chaotic model with sufficient pseudo-creation capability. Recently, chaotic systems and error-correcting codes have gained popularity for generating PRNs and constructing S-boxes for image encryption algorithms.

These approaches have received recognition for their characteristics, such as non-periodicity, responsiveness to input parameters, ergodicity, key sensitivity, and chaotic properties, as mentioned in references [3,18,22–25]. In [26], the authors devised a secure algorithm capable of operating in digital and optical environments. Wang et al. [27] introduced a cryptosystem that leverages diverse techniques like chaotic maps, Fisher-Yates shuffling, and DNA sequence encoding to deliver precise encryption and rapid convergence. Although chaotic maps can generate random sequences quickly, EC structures are more suitable for generating random sequences due to their computational precision [28]. Reyad

et al. [29] developed an idea based on ECs to obtain PRNs that operate effectively in image encryption. Moreover, El-Latif et al. [30] used cyclic ECs and hybrid-chaotic systems to develop an effective image encryption scheme. To generate PRNs, the authors in [3,20] employed an ECs group law operating tool in conjunction with a large prime field, while [2,23] utilized a recursive approach and group law operating tool to identify all points on ECs and generate both S-box and PRNs using algebraic arithmetic operations. However, these techniques can be computationally expensive when working with large prime fields. Using a small fixed prime field may not be effective for generating enough data with strong cryptographic features. Despite attempts to address these challenges, [2] could only produce two strong dynamic S-boxes using a minimum fixed odd prime field. Recently, Farwa et al. [31] proposed constructing the nonlinear component of block cipher by employing EC over binary extension field (BEF) and utilizing the group structure of EC. In [25,26,32,33], the author extended this idea using EC over the Galois field with n equals 8,9 and odd n greater than 9 and utilized the operations of the corresponding Galois field. All the EC-based schemes discussed above use finite fields to achieve the desired level of security. The security of these cryptographic systems, which rely on EC over finite fields, is primarily determined by the computational resources required to solve the discrete logarithm problem. Computers typically perform mathematical operations with binary digits (bits), which can only have two possible values (0 or 1). In the context of cryptography, cryptographic algorithms must be designed to operate on binary data. By performing computations in a BEF, the computational complexity of cryptographic algorithms can be reduced, increasing their efficiency and security.

In this context, we explain two distinct mechanisms that utilize the indexing technique: the S-box method and a collection of PRN streams, each with its unique approach. It is worth mentioning that the S-box construction technique (SCT) generates multiple dynamic S-boxes in 16×16 standard format employing features of BEF. The core sentiment behind SCT is that EC points and operations of the corresponding Galois field jointly equip it. This way, we reduce the time complexity and increase the proposed algorithm's security strength as the computer works in a binary field. Moreover, BEF enables a high degree of parallelism, essential in modern computer architectures. Parallelism allows multiple arithmetic operations to be performed simultaneously, leading to faster computation times. Moreover, the PRN technique is partly utilized by both EC points and basic algebraic operations in a BEF. Due to this, the PRN scheme produces numerous random patterns while ensuring that these patterns are non-repeating and verified. As a result, it is an effective method for achieving diffusion in large-scale multimedia data. Moreover, the findings obtained from implementing both modules confirm the suitability of utilizing SCT and PRN techniques and indexing techniques in various cryptographic protocols.

The rest of the study is structured as follows: Section 2 presents the fundamental principles and discoveries of EC and BEF. Section 3 elucidates the suggested S-box and PRN mechanisms. Section 4 centers on the proposed encryption scheme. Consequently, Section 5 presents the results of simulations conducted on the SCT and proposed encryption scheme. Finally, Section 6 concludes the discussion.

2. Preliminaries

This section covers important concepts such as ECs, Galois fields, Euler's phi function, and primitive polynomials, which are essential and foundational.

2.1. Elliptic curve

For any given prime field F_p, an EC of the form

$$Y^2 = x^3 + ax + b,$$

where a and b are non-zero elements of the corresponding prime field are called weierstrass form of an EC. Also, when we take $a = 0$, then the obtained EC of the form

$$Y^2 = x^3 + b,$$

where $b \neq 0$ is called Mordell elliptic curve (MEC). The specialty of this curve is that it has $p + 1$ points lying on that EC if we take prime field of the form

$$p - 2 \cong 0 \, mod \, 3,$$

where each integer in the field F_p appear once as y-coordinates [34].

2.2. Galois field $GF(2^n)$

Let $\mathbb{R}$ be a commutative ring with identity, with binary operation addition and multiplication. Then $I \subseteq \mathbb{R}$ is called an ideal of $\mathbb{R}$ if

$$a, b \in I \Rightarrow a - b \in I$$

and $aI \subseteq I$ for every $a \in \mathbb{R}$. An ideal in a ring $\mathbb{R}$ denoted as $\mathcal{A} \neq \mathbb{R}$, is considered maximal ideal when no other proper ideal of $\mathbb{R}$ exists that contains $\mathcal{A}$. A commutative ring with an identity whose nonzero elements forms a group under multiplication is called field $\mathbb{F}$. The polynomial ring, denoted by $Z_p[x]$ is a set of polynomials whose coefficients are from the field Z_p. A polynomial $f(x)$ in $Z_p[x]$ is an irreducible polynomial, if it cannot be reduced into the product of lower-degree polynomials in $Z_p[x]$, and the ideal generated by $f(x)$ will be the maximal ideal of the ring $Z_p[x]$ represented as

$$< f(x) >= \{h(x): h(x) = f(x).\, g(x), for\ some\ g(x) \in Z_p[x]\}.$$

The quotient $\frac{Z_p[x]}{<f(x)>}$ is known as Galois field $GF(p^m)$ having p^m elements, where m is the degree of PIP $f(x)$ and p is any prime number. A polynomial

$$f(x) \in GF(p^m)[x]$$

is said to have a PIP of degree m if all its roots are also primitive elements in the corresponding Galois field. Also, addition and subtraction are performed using the corresponding field Z_p. The product of two polynomials in $Z_p[x]$ is equivalent to the remainder obtained from the Euclidean division by p. The extended Euclidean algorithm can compute the multiplicative inverse of any nonzero element. The total number of PIPs of degree n in the binary field is $\frac{\varphi(2^n-1)}{n}$, where φ denotes Euler's phi function.

3. Proposed technique for S-boxes and pseudo-random numbers

In this segment, we suggest a cryptographic algorithm that relies primarily on two distinct

methods of generating random data with a specific length. The precise instructions for each approach are described in subsequent sub-sections.

3.1. S-box construction technique (SCT)

Generating robust and adaptable S-boxes is a critical factor in developing effective cryptographic systems, as they are instrumental in performing nonlinear transformations that evaluate the strength of well-designed crypto-algorithms [35]. Consequently, generating dynamic S-boxes with optimal cryptographic properties is highly desirable in contemporary cryptography. To address the limitations of current S-box constructions and obtain multiple S-boxes, we suggest a rapid technique that employs ECs over the Galois field and their algebraic operations. The subsequent explanation illustrates how the proposed SCT operates.

1) Choose PIP of degree 8 over the binary field

$$\mathrm{P}(t)=t^8+t^5+t^3+t^2+1.$$

Since the number of PIP of degree 8 over the binary field is 16, one can independently choose any other PIP of degree 8.

2) Select an EC $E^{(b,2,8)}$ of the form

$$E^{(b,2,8)}: y^2 = x^3 + b.$$

3) Generate EC points (x, y) by utilizing above equation over the PIP.

4) Apply a bijective map on the points of EC (x, y), such that

$$\pi: E_{x,y}^{(b,2,8)} \to E_x^{(b,2,8)}.$$

Defined by

$$\pi(x, y) = x,$$

where $(x, y) \in E_{x,y}^{(b,2,8)}$.

5) Apply an inverse map under the corresponding BEF

$$\xi: E_x^{(b,2,8)} \to F_{256}.$$

Defined as

$$\xi(x) = \begin{cases} h.x^{-1}, & if\ x \neq 0, \\ h.x, & if\ x = 0, \end{cases}$$

where h be any fixed element of x-coordinates and $x \in E_x^{(b,2,8)}$. Also, inverse is taken under the BEF of order 256 and PIP is taken as mentioned above.

6) For the construction of S-box, further apply a map

$$\xi_\tau: F_{256} \to F_{256},$$

defined as

$$\xi_\tau(x) = r + x,$$

where $r \in F_{256}$ be any non-zero element fixed element and $zr \in F_{256}$. Here $+$ presents

addition over the Galois field $GF(2^8)$.

Since the number of PIP of degree 8 over the binary field is 16, given in Table 1. So, the scheme is capable to generating $16 \times 255 \times 255$ different number of 8×8 S-boxes corresponding to the BEF of degree 8 having optimal NL 112 of each which are given in Table 6. The S-boxes constructed through proposed SCT are depicted in Tables 2–5.

Table 1. PIP and their decimal representation (DR).

PIP	DR	PIP	DR
$t^8+t^4+t^3+t^2+1$	285	$t^8+t^6+t^5+t^4+1$	369
$t^8+t^5+t^3+t^1+1$	299	$t^8+t^7+t^2+t^1+1$	391
$t^8+t^5+t^3+t^2+1$	301	$t^8+t^7+t^3+t^2+1$	397
$t^8+t^6+t^3+t^2+1$	333	$t^8+t^7+t^5+t^3+1$	425
$t^8+t^6+t^4+t^3+t^2+t^1+1$	351	$t^8+t^7+t^6+t^1+1$	451
$t^8+t^6+t^5+t^1+1$	355	$t^8+t^7+t^6+t^3+t^2+t^1+1$	463
$t^8+t^6+t^5+t^2+1$	357	$t^8+t^7+t^6+t^5+t^2+t^1+1$	487
$t^8+t^6+t^5+t^3+1$	361	$t^8+t^7+t^6+t^5+t^4+t^2+1$	501

Table 2. S-box 1 constructed by proposed SCT by choosing parameters $n=8, b=101, h=23, r=11$.

11	20	247	163	117	206	95	67	52	51	154	184	33	159	47	72
28	136	166	21	214	121	221	220	83	171	143	128	222	156	240	160
243	44	185	198	174	48	4	90	150	157	50	41	96	12	147	17
6	135	71	215	251	1	205	167	26	70	228	187	64	86	182	37
119	209	235	114	82	107	158	245	170	219	229	253	255	183	208	207
173	108	133	210	179	226	146	181	189	111	73	92	91	202	39	13
254	38	77	22	45	237	101	34	115	153	14	142	104	106	93	191
217	10	25	199	65	190	30	164	161	218	176	19	23	122	231	151
53	188	102	155	123	138	196	141	212	233	59	78	178	134	116	9
69	118	125	169	192	79	5	63	7	110	165	195	144	62	94	197
88	249	203	16	76	0	148	100	87	177	140	145	180	31	84	244
81	49	32	89	200	230	201	132	186	194	250	172	66	239	55	234
130	204	238	224	40	129	246	15	24	252	120	223	60	56	236	43
8	61	29	213	152	216	35	18	211	137	42	232	57	74	80	103
98	58	248	3	2	68	109	75	46	36	162	126	242	54	175	127
105	27	149	139	85	225	113	227	112	97	124	193	99	131	168	241

Table 3. S-box 2 constructed by proposed SCT by choosing parameters $n = 8, b = 101, h = 23, r = 17$.

17	14	237	185	111	212	69	89	46	41	128	162	59	133	53	82
6	146	188	15	204	99	199	198	73	177	149	154	196	134	234	186
233	54	163	220	180	42	30	64	140	135	40	51	122	22	137	11
28	157	93	205	225	27	215	189	0	92	254	161	90	76	172	63
109	203	241	104	72	113	132	239	176	193	255	231	229	173	202	213
183	118	159	200	169	248	136	175	167	117	83	70	65	208	61	23
228	60	87	12	55	247	127	56	105	131	20	148	114	112	71	165
195	16	3	221	91	164	4	190	187	192	170	9	13	96	253	141
47	166	124	129	97	144	222	151	206	243	33	84	168	156	110	19
95	108	103	179	218	85	31	37	29	116	191	217	138	36	68	223
66	227	209	10	86	26	142	126	77	171	150	139	174	5	78	238
75	43	58	67	210	252	211	158	160	216	224	182	88	245	45	240
152	214	244	250	50	155	236	21	2	230	98	197	38	34	246	49
18	39	7	207	130	194	57	8	201	147	48	242	35	80	74	125
120	32	226	25	24	94	119	81	52	62	184	100	232	44	181	101
171	241	152	71	242	154	44	15	149	214	37	137	67	58	120	96

Table 4. S-box 3 constructed by proposed SCT by choosing parameters $n = 8, b = 101, h = 23, r = 19$.

19	12	239	187	109	214	71	91	44	43	130	160	57	135	55	80
4	144	190	13	206	97	197	196	75	179	151	152	198	132	232	184
235	52	161	222	182	40	28	66	142	133	42	49	120	20	139	9
30	159	95	207	227	25	213	191	2	94	252	163	88	78	174	61
111	201	243	106	74	115	134	237	178	195	253	229	231	175	200	215
181	116	157	202	171	250	138	173	165	119	81	68	67	210	63	21
230	62	85	14	53	245	125	58	107	129	22	150	112	114	69	167
193	18	1	223	89	166	6	188	185	194	168	11	15	98	255	143
45	164	126	131	99	146	220	149	204	241	35	86	170	158	108	17
93	110	101	177	216	87	29	39	31	118	189	219	136	38	70	221
64	225	211	8	84	24	140	124	79	169	148	137	172	7	76	236
73	41	56	65	208	254	209	156	162	218	226	180	90	247	47	242
154	212	246	248	48	153	238	23	0	228	96	199	36	32	244	51
16	37	5	205	128	192	59	10	203	145	50	240	33	82	72	127
122	34	224	27	26	92	117	83	54	60	186	102	234	46	183	103
113	3	141	147	77	249	105	251	104	121	100	217	123	155	176	233

Table 5. S-box 4 constructed by proposed SCT by choosing parameters $n = 8, b = 101, h = 23, r = 23$.

21	10	233	189	107	208	65	93	42	45	132	166	63	129	49	86
2	150	184	11	200	103	195	194	77	181	145	158	192	130	238	190
237	50	167	216	176	46	26	68	136	131	44	55	126	18	141	15
24	153	89	201	229	31	211	185	4	88	250	165	94	72	168	59
105	207	245	108	76	117	128	235	180	197	251	227	225	169	206	209
179	114	155	204	173	252	140	171	163	113	87	66	69	212	57	19
224	56	83	8	51	243	123	60	109	135	16	144	118	116	67	161
199	20	7	217	95	160	0	186	191	196	174	13	9	100	249	137
43	162	120	133	101	148	218	147	202	247	37	80	172	152	106	23
91	104	99	183	222	81	27	33	25	112	187	221	142	32	64	219
70	231	213	14	82	30	138	122	73	175	146	143	170	1	74	234
79	47	62	71	214	248	215	154	164	220	228	178	92	241	41	244
156	210	240	254	54	159	232	17	6	226	102	193	34	38	242	53
22	35	3	203	134	198	61	12	205	151	52	246	39	84	78	121
124	36	230	29	28	90	115	85	48	58	188	96	236	40	177	97
119	5	139	149	75	255	111	253	110	127	98	223	125	157	182	239

Table 6. Experimental results of proposed S-boxes and their comparison.

S-box	NL	BIC	SAC	LP	DP
Proposed-1	112	0.50614	0.503906	0.0625	0.015625
Proposed-2	112	0.50614	0.503906	0.0625	0.015625
Proposed-3	112	0.50614	0.503906	0.0625	0.015625
Proposed-4	112	0.50614	0.503906	0.0625	0.015625
[36]	107.50	0.500419	0.487300	0.1328	0.0390
[2]	107	0.50635	0.499023	0.1250000	0.0390620
[33]	111.25	-	0.487800	0.0703125	0.0234375
[37]	107.25	0.5069	0.502441	0.125	0.039025
[38]	105.5	0.50872	0.535100	0.140625	-
[39]	106.75	-	0.497600	-	0.03906

3.2. PRN generation scheme

PRNs that have been verified are crucial in numerous cryptographic uses, such as data encryption and gambling. To ensure a strong masking effect in data encryption, PRNs are generated using various mathematical structures, including ECs. In this part, instead of using large prime field dependent schemes, we engaged BEF of order n to generate PRNs. The following lines define the proposed algorithm:

1) Choose primitive irreducible polynomials (PIP) $P(t)$ of degree n over the binary field. Since the number of PIP of degree n over the binary field is $\frac{\varphi(2^n-1)}{n}$, one can independently choose any other PIP of degree n.
2) Select an EC $E^{(b,2,n)}$ of the form

$$E^{(b,2,n)}: \mathcal{y}^2 = x^3 + b,$$

here b be any element of the corresponding Galois field excluding zero.

3) Generate EC points $E_{x,\mathcal{y}}^{(b,2,n)}$ by employing equation over given P($\mathcal{t}$).

4) Apply a map on the points of EC points such that

$$T: E_{x,\mathcal{y}}^{(b,2,n)} \to E_x$$

defined by

$$T(x, \mathcal{y}) = x,$$

where $(x, \mathcal{y}) \in E_{x,\mathcal{y}}^{(b,2,n)}$.

5) For the generation of PRN, further apply an inverse map under the corresponding BEF

$$T_1: E_x \to F_n$$

defined as

$$T_1(x) = \begin{cases} \mathcal{w}.x^{-1}, & if\ x \neq 0, \\ \mathcal{w}.x, & if\ x = 0, \end{cases}$$

where $\mathcal{w} \in GF(2^n)\backslash\{0\}$ be any fixed element. Also, inverse is taken under the $GF(2^n)$ and corresponding PIP is utilized.

Since, the irreducible polynomials of degree n that are binary primitives are $\frac{\varphi(2^n-1)}{n}$, where ϕ represents Euler's phi function. So, one can generate $\frac{\varphi(2^n-1)}{n} \times (2^n - 1)$ different number of PRN sequences corresponding to the BEF of degree n using the proposed mechanism.

4. Proposed encryption decryption algorithm

In domains like military, commercial, and medical, images are a form of visual content that requires cautious handling during transmission. Various mathematical frameworks are employed to establish standardized techniques for encrypting images to ensure reliability and safety. Typically, these encryption methods use chaotic and EC systems to create PRNs and S-boxes. This section introduces a novel approach to image encryption that assesses the appropriateness of prospective S-boxes and PRNs for facilitating secure image storage and communication over an insecure channel. Specifically, the proposed method involves encrypting an image I with dimensions of $\mathcal{M} \times \mathcal{N} \times 3$, where $\mathcal{M}$ represents rows and $\mathcal{N}$ represents columns. Also, we use the symbols R, G and B to represent the color components red, green, and blue in an $\mathcal{M} \times \mathcal{N}$ image. When encrypting the image, all three channels are treated as a grayscale image, and each component is encrypted separately. The level of distortion introduced to the image defines the significance of the encryption scheme.

4.1. Encryption scheme

The encryption process involves several steps.

1) Let I denote the color image of pixels $\mathcal{M} \times \mathcal{N} \times 3$, where $\mathcal{M}$ denotes rows and $\mathcal{N}$ denotes columns of the image. Here, 3 denotes the intensities of RGB layers. We work separately on these channels.

2) Since, any two adjacent pixels in the digital image data have strong relationships with one another. To scramble image elements, we take $n = 9$ and the corresponding PIP of the form

$$f(x) = x^9 + x^4 + 1$$

to generate points (x, y) of EC by employing proposed technique (described in Section 3.2). Then use the inclusion map on each both the coordinates of EC points, which is defined as follows:

$$I_{256} : GF(2^9) \to GF(2^8),$$

$$I_{256}(x) = \begin{cases} 0, & if\ x = 0, \\ x, & if\ x \leq 256, \\ 0, & if\ x > 256, \end{cases}$$

$$I_{256}(y) = \begin{cases} 0, & if\ y = 0, \\ y, & if\ y \leq 256, \\ 0, & if\ y > 256. \end{cases}$$

So, after applying this inclusion map, the obtained positive values of x,y coordinates of EC are employed to original image I such that

$$I_p(i, j) = I\big(x(i), y(j)\big),$$

where (i, j) denotes the integer position in the shuffling matrix I_p. Each color component of the image undergoes the permutation process to shuffle the pixels' positions. Consequently, one can get new layers denoted by R_p, G_p and B_p. By applying this process, we get the scrambled image.

3) To enhance the security against chosen plain-text attacks, the substitution step is a crucial component of any cryptographic algorithm. To achieve this, the proposed method incorporates the use of S-boxes generated through the suggested S-box methodology described in Section 3.1. One of the suggested S-boxes is selected for implementation. These S-boxes possess strong cryptographic properties and contribute to the overall strength of the scheme. Following that, the acquired S-boxes are utilized to substitute the scrambled components R_p, G_p and B_p of the image using a technique identical to AES substitution. Consequently, the substituted components R_s, G_s and B_s can be obtained.

4) The generation of PRNs holds great significance in multiple multimedia data protection applications. Numerous schemes for generating random numbers have been investigated in the research. Among them, EC is commonly employed for random number generation. In this section, a sequence of random numbers ψ is generated by selecting an appropriate value for n such that $2^n \geq M \times W$, ensuring the diffusion of encrypted data through the proposed technique (explained in Section 3.2). Consequently, take $M \times W$ number of elements ψ_r from that sequence and reduce the size of elements of that sequence in the range of image bits. In this part, we take $n = 16$ and the corresponding PIP of the form

$$f(x) = x^{16} + x^5 + x^3 + x^2 + 1$$

to generate PRNs sequence ψ by employing proposed technique (described in Section 3.2). Further, apply mode operation to the elements of sequence ψ and covert them in the range of 256 order Galois field

$$F_{256} : GF(2^{16}) \to GF(2^8)$$

defined as

$$F_{256}(s) = s \; mod \; 256,$$

where $s \in \psi$. The reduced sequence ψ_r are then utilized for the diffusion phase using the below equations

$$R_E = R_s(i) + \psi_r(i),$$

$$G_E = G_s(i) + \psi_r(i),$$

$$B_E = B_s(i) + \psi_r(i),$$

where R_E, G_E, and B_E are the encrypted pixel values for the red, green, and blue channels, respectively, and $\psi_r(i)$ is the i_{th}-byte in PRNs stream ψ_r. $R_s(i), G_s(i)$ and $B_s(i)$ is the i_{th}-byte in RGB channels R_s, G_s, and B_s respectively. Eventually, blend these components of the image, which is required ciphered image.

In this study, we tested the color image of women, house, jellybeans, and couple of dimensions 256×256. The decryption process of the proposed algorithm is same as the encryption process but with the inverse order of operations. The flowchart of proposed algorithm is also depicted in Figure 1. Further, the outcomes and analyses are presented in the subsequent section.

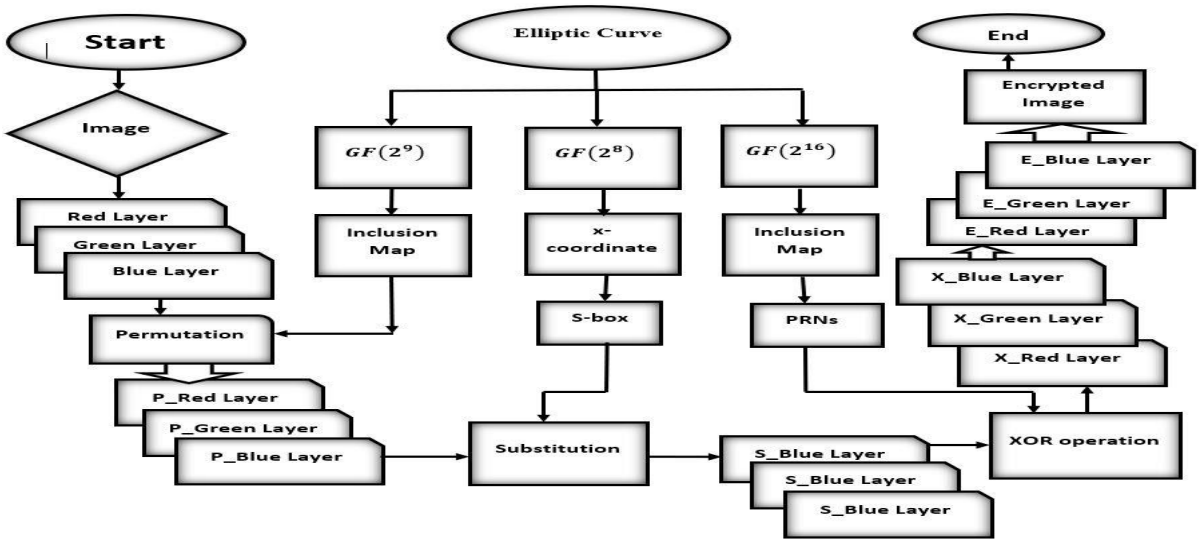

Figure 1. Flowchart of proposed algorithm.

4.2. Decryption scheme

In this subsection, we discussed the process of image decryption in detail. First, we take the cipher image obtained from the encryption process defined in the previous subsection. Then, we divide the image into RGB channels and XORed with the generated sequence, which each channel is applied in the encryption scheme. Further, substitute inverse S-boxes with each channel as we did in the encryption scheme. Moreover, an inverse permutation on each coordinate of 2) in Section 4.1 is applied to the obtained image to get the plain image.

5. Security and performance analyses

If an encryption algorithm passes several security tests and meets specific standards, it is deemed suitable for practical use. In this research, we evaluated the effectiveness of a proposed cryptosystem by encrypting different color images, such as women, house, jellybeans, and couple, shown in Figure 2. Following the encryption process, the encrypted images underwent several performance tests. These tests, which will be elaborated on in the upcoming subsection, strived to evaluate their stability against assorted attacks.

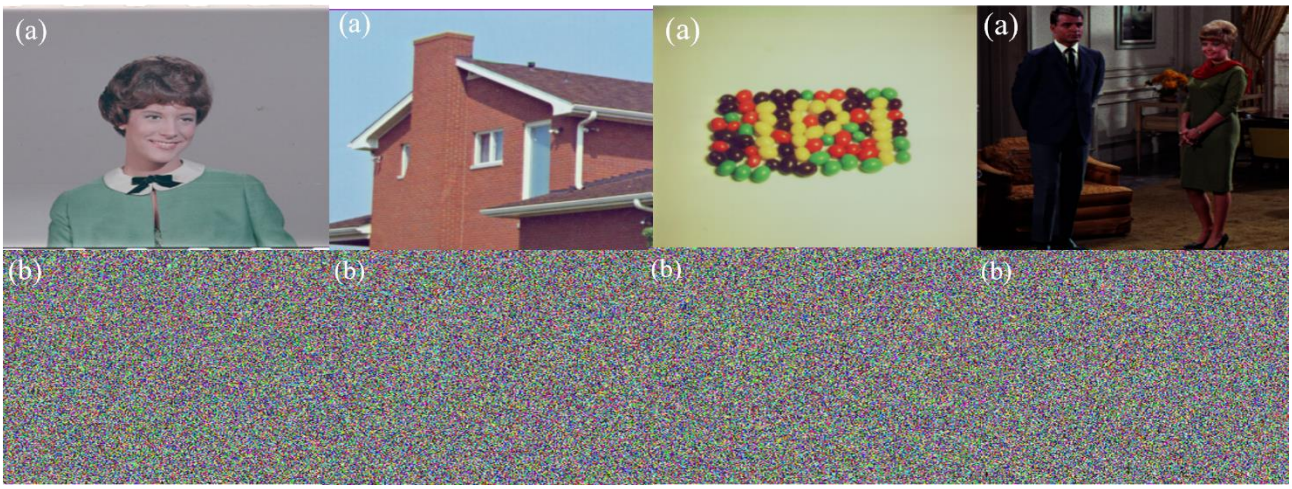

Figure 2. Original and ciphered images: (a) the original images of women, house, jellybeans, and couple; (b) ciphered images.

5.1. Performance analysis of the generated S-box

The cryptographic strength of the S-boxes developed for the encryption procedure is evaluated using established metrics such as nonlinearity (NL), strict avalanche criteria (SAC), linear branch number (LBN), differential branch number (DBN), bit independence criteria (BIC), linear approximation probability (LP), differential approximation probability (DP), balance, and linear structure (LS). These assessments are commonly employed to gauge the effectiveness of S-boxes. The ensuing results present the performance index of the generated S-boxes.

5.1.1. NL

The NL of a Boolean function f refers to the minimum Hamming distance between the set of all affine Boolean functions and f. We denoted the nonlinearity off f by N_f and mathematically it can be defined as

$$N_f = \min\{d(f,h): h \in A\},$$

where A is the set of all affine Boolean functions and N_f denotes the hamming distance between f and h. The maximum NL score of $n \times n$ S-box can have $2^{n-1} - 2^{\frac{n}{2}-1}$.

Thus, in the case for $n = 8$, the maximum possible NL score is 120. Also, the proposed S-boxes

have an optimal NL score of 112 depicted in Table 6.

5.1.2. SAC

The notions of completeness and avalanche were created by Webster and Tavares in 1985, who also detailed the analysis of the SAC. This criterion was investigated to see how the output bits performed when the input bits underwent alterations. Also, one can claim that the SAC criterion is satisfied if all SAC matrix entries are located within a small neighborhood of 0.5. Table 6 displays the SAC outcome of the suggested S-boxes and their comparison to various existing schemes. As a result, the proposed S-boxes met the requirements of the sac test.

5.1.3. BIC

In 1985, Webster and Tavares also provided the significant Boolean function property known as the BIC. The individual bits generated by the eight-constitution function are compared using the BIC. This criterion assesses the correlation between the n_{th} and m_{th} output bits if the ith input bit undergoes a little change. An S-box is deemed to meet the BIC requirements if the entries of its BIC matrix are near 0.5. The different proposed and existing S-boxes are put to the BIC test. The BIC result of the proposed S-boxes and some existing S-boxes is shown in Table 6.

5.1.4. LP

The LP analysis is used to determine the scheme's maximum imbalance value. We assign B_i and B_o to the input and output masks, respectively. The sequence of equal output bits chosen by mask B_o is comparable to the equality of the input bits selected by mask B_i, according to Matsui's definition of LP, defined mathematically as follows:

$$LP = max_{Bi,B_o \neq 0} \left| \frac{\{\# \ i \in Y | i.B_i = S(i).B_0\}}{2^n} - \frac{1}{2} \right|,$$

where Y stands for the set input bits of order 2^n. The performance results of the LP analysis are shown in Table 6, indicating that the suggested S-boxes successfully resist linear cryptanalysis.

5.1.5. DP

The value of DP is calculated using the differential uniformity of the S-box, which is defined as:

$$DP(\delta u \to \delta v) = \frac{\{u \in X | f(u) \otimes f(u + \delta u) = \delta v\}}{2^n}.$$

This indicates that each input differential δu corresponds to a unique output differential δv, ensuring a uniform probability mapping for each i. The DP analysis of the S-boxes produced using the proposed construction approach indicates that the resulting values are close to the ideal value, as presented in Table 6.

5.1.6. Balance

The Boolean function is said to be balanced when there is an equal chance of both 0 and 1

appearing as the output of the Boolean function after all input variable possibilities have been considered. Table 7 depicts that every S-box of the proposed scheme has that property.

Table 7. Experimental results of proposed S-boxes.

S-box	LBN	DBN	Balance	LS
Proposed-1	2	2	Yes	0
Proposed-1	2	2	Yes	0
Proposed-1	2	2	Yes	0
Proposed-1	2	2	Yes	0

5.1.7. Differential and linear branch number

The DBN of an $n \times n$ matrix M is a mapping $\varphi: (\{0,1\}^m)^n \longrightarrow (\{0,1\}^m)^n$ defined as

$$\beta_d(M) = \min\{wt(a) + wt(M.a^T)|,\ a \in (\{0,1\}^m)^n, a \neq 0\}.$$

The S-box has an input and output size of m-bits each, and the number of S-boxes in a diffusion layer is represented by n arranged in a matrix M. Furthermore, wt denotes the hamming weight of a codeword which gives us the nonzero vectors in that codeword [16]. On the other hand, in LBN, instead of using matrix M, the transpose of that matrix is engaged as defined below

$$\psi_{lbn}(S_b) = \min_{g,g' \in F_2^n : cc(g,g') \neq 0} (\{wt(g) + wt(g')\}),$$

where $cc(g, g')$ presents the coefficient of auto correlation. Additionally, DBN is associated with the difference distribution table, whereas LBN is related to the correlation matrix. The proposed S-boxes LBN and DBN values are presented in Table 7.

5.1.8. LS

The cryptographic significance of the S-boxes LS is examined to ensure its robustness against attacks. It has been observed that block ciphers with linear techniques can be vulnerable to attacks that are faster than an exhaustive key search. Therefore, the confusion phase of the block cipher must avoid any LSs. The LS of an S-box is determined by the following mathematical expression

$$g(x) + g(x + a) = C,$$

where

$$g(x) \in {F_2}^n \ \forall\ x \in {F_2}^n$$

and for some $a \in {F_2}^n$ and $C \in F_2$. The LS of an S-box is defined by its Boolean function C. If C is equal to zero, the LS is known as an invariant LS. If C is equal to one, the LS is known as a complementary LS. Table 7 demonstrates that the proposed S-boxes possess no LS, making them suitable for cryptographic purposes.

5.2. Security performance of the proposed image encryption technique

In this part, several well-known security tests are used to evaluate the proposed encryption system's level of security. We used images of women, house, jellybeans, and couple for encryption.

5.2.1. Histogram analysis

An image histogram visualizes the distribution of grayscale frequencies within an image, offering insights into its tonal distribution. When applying the suggested technique for image encryption, the frequency of occurrence for each grayscale value in the encrypted image tends to become more uniform, resulting in a flatter histogram. This indicates that the encryption method is highly resistant to traditional statistical attacks. The corresponding images and their histograms are illustrated in Figure 3, the findings indicate that the histograms of the encrypted images exhibit a nearly uniform distribution and differ significantly from those of the original images. This observation suggests that the proposed scheme demonstrates high resilience against statistical attacks.

5.2.2. Information entropy

The amount of unpredictability and uncertainty of the gray-scale values in the encrypted image is calculated using information entropy. The appropriate entropy score is 8 bits because the encrypted image data's numeric range is 0 to 255. As a result, the encrypted image is increasingly resistant to popular statistical attacks, the closer it comes to 8 bits. The higher entropy value of the proposed scheme can be attributed to its ability to generate more random encrypted data. This randomness makes it difficult for an attacker to determine the original image from the encrypted data. As a result, the proposed scheme can efficiently resist statistical analysis, making it a suitable choice for various security applications. Overall, the results presented in Table 8 indicate that the proposed scheme has higher entropy.

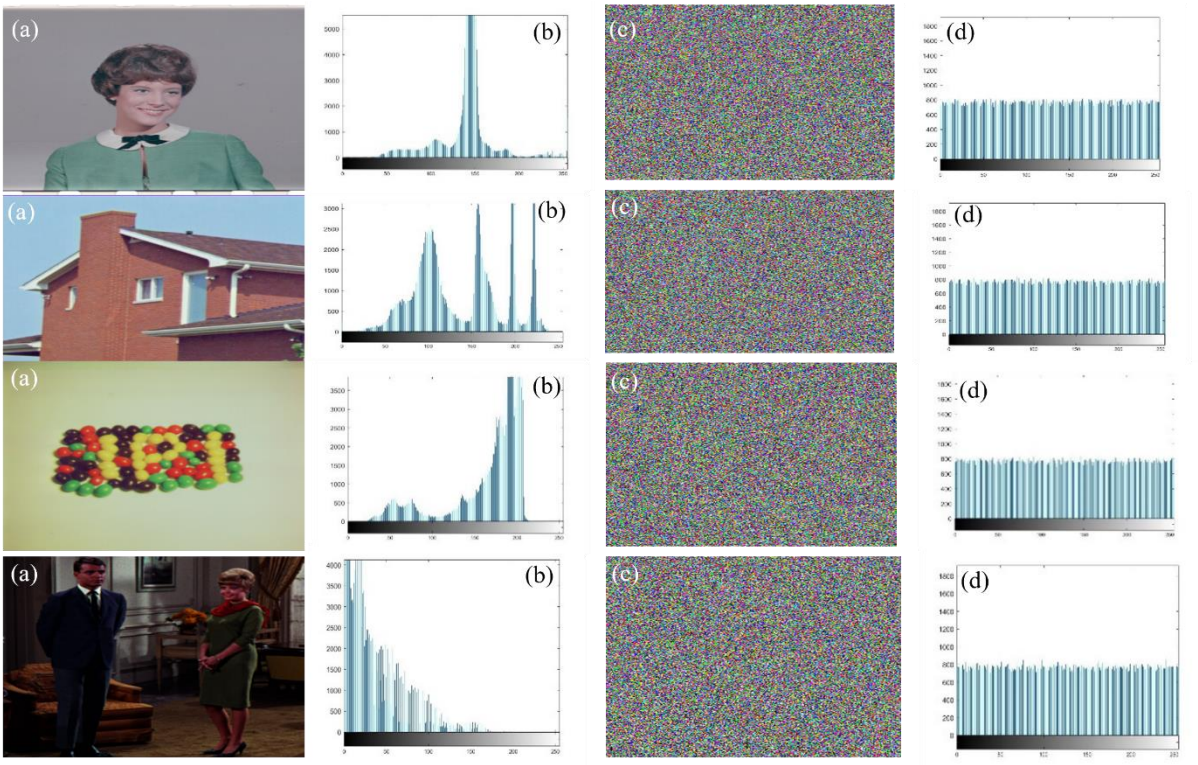

Figure 3. Histograms of original images and ciphered images: (a) the original images: Women, house, jellybeans, and couple; (b) the histograms of the original images; (c) the ciphered images; (d) the histograms of the ciphered images.

Table 8. Comparison of the entropy results of the ciphered images.

Scheme	Images	Entropy
-	Women	7.9991
Proposed scheme	House	7.9990
-	Jellybeans	7.9990
-	Couple	7.9991
[40]	Lena	7.9970
-	Cameraman	7.9848
[41]	Lena	7.9970
[42]	Lena	7.9962
-	Baboon	7.9971
[43]	Lena	7.9970
-	Baboon	7.9969

5.2.3. Contrast

The contrast ratio, which helps the viewer recognize the object in the image, is one of the key aspects of image quality. Contrast analysis determines how much contrast there is between adjacent pixels over the entire image. The encryption method is deemed to pass the contrast test if the contrast ratio in the ciphered image is increased. The following is a list of the contrast coefficient's mathematical representations:

$$CA = \sum_{i,j} \frac{Q(i,j)}{1+|i+j|},$$

where $Q(i,j)$denotes the number of gray level co-occurrence matrices of the image. Also, the constant image has a contrast value of zero. The contrast score of the encrypted image is approximately 10.49 presented in Table 9, indicating a significant variation in pixel intensity and its adjacent pixels throughout the entire image.

Table 9. Statistical analysis: (a) original images, (b) encrypted images and (c) existing schemes encrypted images.

Images	Contrast	Energy	Homogeneity
a. Women	0.0804	0.4304	0.9688
b. Encrypted	10.4684	0.0156	0.3896
a. Home	0.2042	0.1945	0.9053
b. Encrypted	10.4733	0.0156	0.3893
a. Jellybeans	0.1279	0.3412	0.9441
b. Encrypted	10.4861	0.0156	0.3906
a. Couple	0.2084	0.2637	0.9172
b. Encrypted	10.5344	0.0156	0.3884
c. [3]	10.4148	0.0156	0.3887
c. [36]	10.5716	0.0156	0.3865
c. [32]	9.9954	0.0157	0.3908
c. [33]	9.99240	0.0156	0.3887

5.2.4. Energy

The gray level co-occurrence matrices of the encrypted image are required for analyzing the

images energy. The square root of the angular second moment is used in energy analysis to determine the uniformity of pixel intensities. The energy is calculated using the mathematical equation provided below:

$$EA = \sum_{i,j} Q(i,j)^2,$$

whereas $Q(i,j)$ represents GLCM. The low homogeneity score of the encrypted images indicates a higher difference in the GLCM.

5.2.5. Homogeneity

We focus on assessing the GLCM, which is also known as a grey-tone spatial dependency matrix, to determine the proximity of dispersed elements in images to the GLCM diagonal. This is because images inherently contain dispersed contents when captured. The equation utilized for analyzing homogeneity is expressed mathematically as

$$HA = \sum_i \sum_j \frac{Q(i,j)}{1 - |i + j|}.$$

The homogeneity score for the encrypted images is very low, which suggests that the difference in the GLCM is higher.

5.2.6. Correlation

There is a strong correlation between adjacent pixels in color images due to their close values. The correlation coefficient measures the linearity between neighboring pixel values in the vicinity. The primary objective of the encryption method is to distort the pixels to minimize the correlation among adjacent pixels in the image. For an image encryption algorithm to be considered robust and suitable for security purposes, the correlation coefficient of the encrypted image should approach zero. The experimental results of the correlation test, conducted on various plain and encrypted images for each color channel, are presented in Table 10. The correlation coefficient values obtained from the test indicate that the proposed encryption scheme is highly effective and resilient against statistical attacks. Additionally, the correlation plots depicted in Figure 4 provide evidence of the effectiveness of the proposed approach.

Table 10. Correlation analysis of original and encrypted images.

Image	Horizontal	Vertical	Diagonal
Women	0.9710	0.9355	0.9162
Encrypted-women	0.0432	0.0057	0.0245
Home	0.9816	0.9601	0.9477
Encrypted-home	-0.0210	0.0028	-0.0042
jellybeans	0.9825	0.9836	0.9694
Encrypted-jellybeans	0.0277	0.0004	0.0041
Couple	0.9217	0.9592	0.9223
Encrypted-couple	0.0212	0.0073	-0.0054

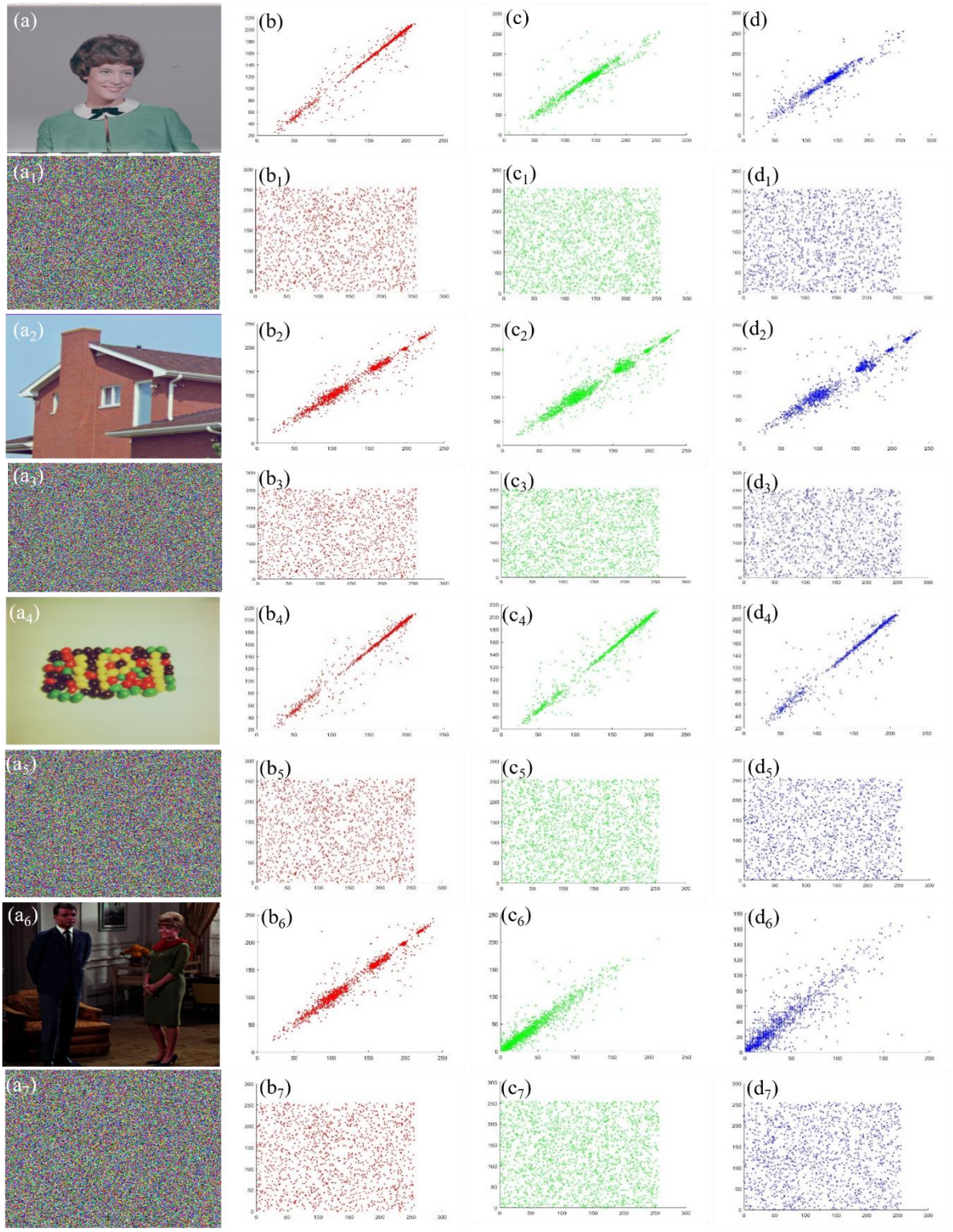

Figure 4. Correlation plots of (a) women original image; (b, c, d) adjacent pixels of rgb channels of the original color image women; similarly (a_1) women encrypted image; (b_1, c_1, d_1) adjacent pixels of rgb channels of the women encrypted image; (a_2) home original image; (b_2, c_2, d_2) rgb channel plots; (a_3) home encrypted image; (b_3, c_3, d_3) rgb channel plots; (a_4) jellybeans original image; (b_4, c_4, d_4) rgb channel plots; (a_5) jellybeans encrypted image; (b_5, c_5, d_5) rgb channel plots; (a_6) couple original image; (b_6, c_6, d_6) rgb channel plots; (a_7) couple encrypted image; (b_7, c_7, d_7) rgb channel plot.

5.2.7. Differential attacks

Attackers commonly employ the differential attack method, where they seek to detect patterns in the encrypted data generated by two nearly identical plain inputs. If such a pattern exists, the attacker may exploit it to uncover the precise key or exploit a vulnerability in the encryption algorithm's security A secure encryption technique creates encrypted data that appears almost random, even when there is a minor change in the input data, as a barrier against differential assaults. The unified average changing intensity (UACI) and the number of pixels change rates (NPCR) are the relevant metrics to assess the encryption scheme's susceptibility to differential attacks. These findings illustrate the strong correlation between the suggested encryption method and the original image data, which could enhance its resilience to differential attacks. Table 11 assesses various color images with their respective NPCR and UACI scores measured. The proposed encryption approach scored higher than the optimal value of 99.58% for NPCR, while the UACI scores were within the optimal range of [33.3% to 33.5%]. These results imply that the proposed encryption method relies heavily on the original image data and has the potential to be more effective against differential attacks.

Table 11. Comparison of NPCR and UACI analysis with existing schemes.

Scheme	NPCR	UACI
-	99.6318	33.4281
Proposed	99.5972	33.4706
-	99.6175	33.4421
-	99.6023	33.4634
[44]	99.6067	33.5000
[45]	99.6233	33.6733
[46]	99.5681	33.4067
[47]	99.6000	33.3867

5.2.8. Mean square error (MSE)

The MSE stands out as a widely used metric for quantifying the discrepancy between the original and encrypted images, thereby evaluating the efficacy between the pixels of the plain image and the corresponding pixel in the encrypted image for all pixels in the image. The resulting squared errors are summed and divided by the total number of pixels. Notably, greater MSE values indicate increased robustness of an encryption algorithm against statistical attacks.

5.2.9. Peak signal to noise ratio (PSNR)

Utilizing the MSE as a foundation, the PSNR emerges as an additional performance measure for assessing encryption algorithms. As given by the following equation, PSNR is determined by taking the logarithm of the ratio between the square of the maximum pixel value (typically 255) and the MSE. As PSNR and MSE display an inverse relationship, diminished PSNR values signify enhanced robustness of an encryption algorithm

$$PSNR = 10log\left(\frac{I_{max}^2}{MSE}\right).$$

Presented in Table 12 are the outcomes for both MSE and PSNR achieved through our newly proposed encryption algorithm across various images. Furthermore, we provide a comparison with the latest literature in Table 12, focusing on MSE and PSNR, respectively. Notably, the findings indicate that our proposed algorithm exhibits superior MSE and PSNR values when compared to [48,49].

Table 12. Comparison of MSE and PSNR values of the proposed scheme with existing schemes of plain-encrypted (PE) and plain-decrypted (PD) images.

Images	MSE_{PE}	MSE_{PD}	$PSNR_{PE}$	$PSNR_{PD}$
Women	3930.7	0	12.1861	∞
Home	8344.7	0	8.9167	∞
Jellybeans	7375.2	0	9.4531	∞
Couple	8909.9	0	8.6321	∞
[48]	40.264	0	9.1244	∞
[49]	7952.7	0	9.1812	∞

5.2.10. Resistant to cryptographic attacks

In the proposed scheme, an algorithm for image encryption is designed to combine an elliptic curve and arithmetic operations of a BEF and an invertible function under the Galois field. This algorithm has been designed to resist various attacks, including chosen-plaintext and chosen-ciphertext attacks. Since a robust encryption algorithm integrates confusion and diffusion properties to fortify its security measures. In the proposed algorithm, we employed permutation to disperse the pixels of images. Further, we generate the nonlinear component by utilizing EC over BEF and inverse function, introducing complexity and preventing simple algebraic relationships between the plain and obtained image. Further, the invertible function under the Galois field provides diffusion to ensure that any changes made to the ciphertext will significantly impact the decrypted image. Additionally, the key stream is generated by utilizing the points of EC and operations of the Galois field; the generated key stream is then XORed with the image entries. The randomness of the key stream ensures that the XOR operation is not easily predictable, enhancing the security of the encryption. The pseudo-randomness of PRNs helps prevent attackers from exploiting regularities or biases in the encryption process. Using these three cryptographic primitives in combination provides a high level of security and makes it difficult for an attacker to break the encryption.

Additionally, using the complex structure of EC and operations of BEF ensures that the algorithm resists attacks. Collectively, these inherent properties impose significant challenges for potential attackers attempting to deduce information about the encryption key or plaintext from the ciphertext. Overall, this proposed algorithm is a robust and effective method for image encryption that provides resistance to various attacks. With the increasing importance of secure image transmission in today's digital world, this algorithm is an essential contribution to the field of cryptography.

5.2.11. Complexity analysis

The complexity analysis involves assessing the resources, such as time and memory, required for execution. Various methods exist to determine algorithmic complexity, the most common being big "O" notation. In this section, we evaluated the proposed scheme using big O. Given that the scheme functions as a substitution permutation network, it initially generates S-boxes, employing them for

substitution in the encryption process. Subsequently, the generated numbers are utilized in the permutation module, which linearly shuffles image data. Consequently, the permutation module's time complexity for data permutation is $O(3\times M\times N)$. Similarly, substituting fixed pixels within the permutation module also requires constant time. In summary, the overall time complexity of the proposed algorithm is $O(3\times M\times N)$.

6. Conclusions

EC structure is commonly employed in image encryption applications. In this article, we designed a technique to protect RGB images while transmitting them through insecure channels. The proposed scheme employs a three-phase mechanism to encrypt data. In the first phase, each pixel value is dispersed using a piecewise function on EC points, while in the second phase, the proposed S-box is utilized to create confusion in the image. Subsequently, a PRNS is generated and applied to the confused image to achieve the desired diffusion. The key elements of this proposed image encryption technique include the following: Both SCT and PRNS are designed by utilizing the properties of BEF on EC points. Instead of using large primes, a novel technique is employed for both SCT and PRNS. BEF can resist side-channel attacks, a security attack that exploits information leaked during a cryptographic operation. Because BEF has a uniform distribution of values, which makes it difficult for attackers to obtain sensitive information, BEF can designate large numbers compactly, which is helpful in applications requiring efficient data storage and transmission.

Regarding security analysis, the proposed scheme is up to the mark. Using various testing tools, we assessed the effectiveness of the proposed SCT and determined that it exhibits greater efficiency relative to its respective features. Moreover, standardized tests are performed on the encrypted image data to evaluate the encryption performance. The results of the simulations indicate that the proposed modules generate encrypted data that is highly resistant to typical attacks. Furthermore, a comparative analysis between our scheme and recent research demonstrates that our approach requires fewer operations than existing schemes. From a futuristic point of view, we can also extend this algorithm to the general algorithm.

Use of AI tools declaration

The authors declare that they have not used Artificial Intelligence (AI) tools in the creation of this article.

Acknowledgments

The authors extend their gratitude to the deanship of Scientific research at King Khalid University for funding this work through the research group’s program under grant number R.G.P.2/5/44.

Conflict of interest

The authors declare that they have no conflicts of interest.

References

1. Y. Xian, X. Wang, Fractal sorting matrix and its application on chaotic image encryption, *Inf. Sci.*, **547** (2021), 1154–1169. https://doi.org/10.1016/j.ins.2020.09.055
2. M. I. Haider, A. Ali, D. Shah, T. Shah, Block cipher's nonlinear component design by elliptic curves: an image encryption application, *Multimedia Tools Appl.*, **80** (2021), 4693–4718. https://doi.org/10.1007/s11042-020-09892-5
3. S. Ibrahim, A. M. Abbas, Efficient key-dependent dynamic S-boxes based on permutated elliptic curves, *Inf. Sci.*, **558** (2021), 246–264. https://doi.org/10.1016/j.ins.2021.01.014
4. A. A. A. El-Latif, B. Abd-El-Atty, M. Amin, A. M. Iliyasu, Quantum-inspired cascaded discrete-time quantum walks with induced chaotic dynamics and cryptographic applications, *Sci. Rep.*, **10** (2020), 1930. https://doi.org/10.1038/s41598-020-58636-w
5. M. M. Hazzazi, H. U. Rehman, T. Shah, H. Younas, Asymmetric key cryptosystem for image encryption by elliptic curve over Galois field, *Comput. Mater. Con.*, **76** (2023), 2033–2060. https://doi.org/10.32604/cmc.2023.040629
6. H. U. Rehman, M. M. Hazzazi, T. Shah, Z. Bassfar, D. Shah, An efficient audio encryption scheme based on elliptic curve over finite fields, *Mathematics*, **11** (2023), 3824. https://doi.org/10.3390/math11183824
7. H. Wen, Y. Lin, Z. Xie, T. Liu, Chaos-based block permutation and dynamic sequence multiplexing for video encryption, *Sci. Rep.*, **13** (2023), 14721. https://doi.org/10.1038/s41598-023-41082-9
8. A. H. Zahid, E. Al-Solami, M. Ahmad, A novel modular approach based substitution-box design for image encryption, *IEEE Access*, **8** (2020), 150326–150340. https://doi.org/10.1109/ACCESS.2020.3016401
9. S. Ibrahim, A. Alharbi, Efficient image encryption scheme using Henon map, dynamic S-boxes and elliptic curve cryptography, *IEEE Access*, **8** (2020), 194289–194302. https://doi.org/10.1109/ACCESS.2020.3032403
10. J. Brown, J. F. Zhang, B. Zhou, M. Mehedi, P. Freitas, J. Marsland, et al., Random-telegraph-noise-enabled true random number generator for hardware security, *Sci. Rep.*, **10** (2020), 17210. https://doi.org/10.1038/s41598-020-74351-y
11. P. Ayubi, S. Setayeshi, A. M. Rahmani, Deterministic chaos game: a new fractal based pseudo-random number generator and its cryptographic application, *J. Inf. Secur. Appl.*, **52** (2020), 102472. https://doi.org/10.1016/j.jisa.2020.102472
12. Y. Wang, Z. Liu, J. Ma, H. He, A pseudorandom number generator based on piecewise logistic map, *Nonlinear Dyn.*, **83** (2016), 2373–2391. https://doi.org/10.1007/s11071-015-2488-0
13. Q. Lu, C. Zhu, X. Deng, An efficient image encryption scheme based on the LSS chaotic map and single S-box, *IEEE Access*, **8** (2020), 25664–25678. https://doi.org/10.1109/ACCESS.2020.2970806
14. H. Wen, Z. Xie, Z. Wu, Y. Lin, W. Feng, Exploring the future application of UAVs: face image privacy protection scheme based on chaos and DNA cryptography, *J. King Saud Univ.*, **36** (2024), 101871. https://doi.org/10.1016/j.jksuci.2023.101871
15. H. Wen, Y. Lin, S. Kang, X. Zhang, K. Zou, Secure image encryption algorithm using chaos-based block permutation and weighted bit planes chain diffusion, *iScience*, **27** (2024), 108610. https://doi.org/10.1016/j.isci.2023.108610
16. W. Feng, X. Zhao, J. Zhang, Z. Qin, J. Zhang, Y. He, Image encryption algorithm based on plane-level image filtering and discrete logarithmic transform, *Mathematics*, **10** (2022), 2751. https://doi.org/10.3390/math10152751

17. H. Wen, S. Kang, Z. Wu, Y. Lin, Y. Huang, Dynamic rna coding color image cipher based on chain feedback structure, *Mathematics*, **11** (2023), 3133. https://doi.org/10.3390/math11143133
18. H. S. Alhadawi, D. Lambic, M. F. Zolkipli, M. Ahmad, Globalized firefly algorithm and chaos for designing substitution box, *Inf. Secur. Appl.*, **55** (2020), 102671. https://doi.org/10.1016/j.jisa.2020.102671
19. A. Razaq, A. Ullah, H. Alolaiyan, A. Yousaf, A novel group theoretic and graphical approach for designing cryptographically strong nonlinear components of block ciphers, *Wireless Pers. Commun.*, **116** (2021), 3165–3190. https://doi.org/10.1007/s11277-020-07841-x
20. S. Toughi, M. H. Fathi, Y. A. Sekhavat, An image encryption scheme based on elliptic curve pseudo random and advanced encryption system, *Signal Process.*, **141** (2017), 217–227. https://doi.org/10.1016/j.sigpro.2017.06.010
21. Y. Lu, K. Yu, X. Lv, Image encryption with one-time password mechanism and pseudo-features, *Multimedia Tools Appl*., **1** (2021), 15041–15055. https://doi.org/10.1007/s11042-021-10522-x
22. X. Wang, N. Guan, H. Zhao, S. Wang, Y. Zhang, A new image encryption scheme based on coupling map lattices with mixed multi-chaos, *Sci. Rep.*, **10** (2020), 9784. https://doi.org/10.1038/s41598-020-66486-9
23. Q. Liu, L. Liu, Color image encryption algorithm based on DNA coding and double chaos system, *IEEE Access*, **8** (2020), 83596–83610. https://doi.org/10.1109/ACCESS.2020.2991420
24. F. Özkaynak, Construction of robust substitution boxes based on chaotic systems, *Neural Comput. Appl*., **31** (2019), 3317–3326. https://doi.org/10.1007/s00521-017-3287-y
25. T. Ye, L. Zhimao, Chaotic S-box: six-dimensional fractional Lorenz-Duffing chaotic system and O-shaped path scrambling, *Nonlinear Dyn.*, **94** (2018), 2115–2126. https://doi.org/10.1007/s11071-018-4478-5
26. S. S. Yu, N. R. Zhou, L. H. Gong, Z. Nie, Optical image encryption algorithm based on phase-truncated short-time fractional Fourier transform and hyper-chaotic system, *Opt. Lasers Eng.*, **124** (2020), 105816. https://doi.org/10.1016/j.optlaseng.2019.105816
27. X. Wang, Y. Li, Chaotic image encryption algorithm based on hybrid multi-objective particle swarm optimization and DNA sequence, *Opt. Lasers Eng.*, **137** (2021), 106393. https://doi.org/10.1016/j.optlaseng.2020.106393
28. N. Jia, S. Liu, Q. Ding, S. Wu, X. Pan, A new method of encryption algorithm based on chaos and ECC, *J. Inf. Hiding Multimedia Signal Process*., **7** (2016), 637–643. https://doi.org/10.1016/j.optlaseng.2015.356643
29. O. Reyad, Z. Kotulski, W. M. Abd-Elhafiez, Image encryption using chaos-driven elliptic curve pseudo-random number generators, *Appl. Math. Inf. Sci.*, **10** (2016), 1283–1292. https://doi.org/10.18576/amis/100407
30. A. A. Abd El-Latif, X. Niu, A hybrid chaotic system and cyclic elliptic curve for image encryption, *AEU Int. J. Electron. Commun*., **67** (2013), 136–143. https://doi.org/10.1016/j.aeue.2012.07.004
31. S. Farwa, A. Sohail, N. Muhammad, A novel application of elliptic curves in the dynamical components of block ciphers, *Wireless Pers. Commun.*, **115** (2020), 1309–1316. https://doi.org/10.1007/s11277-020-07628-0
32. H. U. Rehman, T. Shah, A. Aljaedi, M. M. Hazzazi, A. R. Alharbi, Design of nonlinear components over a mordell elliptic curve on Galois fields, *Comput. Mater. Continua*, **71** (2022), 1313–1329. https://doi.org/10.32604/cmc.2022.022224
33. H. U. Rehman, T. Shah, M. M. Hazzazi, A. Alshehri, B. Zaid, Mrdell elliptic curve based design of nonlinear component of block cipher, *Comput. Mater. Continua*, **73** (2022), 2913–2930. https://doi.org/10.32604/cmc.2022.028765
34. L. C. Washington, *Elliptic curves: number theory and cryptography*, CRC Press, 2008.

35. X. Lai, J. L. Massey, A proposal for a new block encryption standard, *Advances in Cryptology-EUROCRYPT'90: Workshop on the Theory and Application of Cryptographic Techniques Aarhus, Denmark*, 1990, 389–404. https://doi.org/10.1007/3-540-46877-3_35
36. M. I. Haider, T. Shah, A. Ali, D. Shah, I. Khalid, An innovative approach towards image encryption by using novel PRNs and S-boxes modeling techniques, *Math. Comput. Simul.*, **209** (2023), 153–168. https://doi.org/10.1016/j.matcom.2023.01.036
37. M. Ramzan, T. Shah, M. M. Hazzazi, A. Aljaedi, A. R. Alharbi, Construction of S-boxes using different maps over elliptic curves for image encryption, *IEEE Access*, **9** (2021), 157106–157123. https://doi.org/10.1109/ACCESS.2021.3128177
38. Z. Hua, J. Li, Y. Chen, S. Yi, Design and application of an S-box using complete Latin square, *Nonlinear Dyn.*, **104** (2021), 807–825. https://doi.org/10.1007/s11071-021-06308-3
39. Z. Jiang, Q. Ding, Construction of an S-box based on chaotic and bent functions, *Symmetry*, **13** (2021), 671. https://doi.org/10.3390/sym13040671
40. Z. E. Dawahdeh, S. N. Yaakob, R. R. bin Othman, A new image encryption technique combining elliptic curve cryptosystem with hill cipher, *J. King Saud Univ.*, **30** (2018), 349–355. https://doi.org/10.1016/j.jksuci.2017.06.004
41. C. K. Volos, I. M. Kyprianidis, I. N. Stouboulos, Image encryption process based on chaotic synchronization phenomena, *Signal Process.*, **93** (2013), 1328–1340. https://doi.org/10.1016/j.sigpro.2012.11.008
42. X. Wang, C. Liu, D. Xu, C. Liu, Image encryption scheme using chaos and simulated annealing algorithm, *Nonlinear Dyn.*, **1** (2016), 1417–1429. https://doi.org/10.1007/s11071-015-2579-y
43. X. Wei, L. Guo, Q. Zhang, J. Zhang, S. Lian, A novel color image encryption algorithm based on DNA sequence operation and hyper-chaotic system, *J. Syst. Software*, **85** (2012), 290–299. https://doi.org/10.1016/j.jss.2011.08.017
44. X. Chai, X. Fu, Z. Gan, Y. Lu, Y. Chen, A color image cryptosystem based on dynamic DNA encryption and chaos, *Signal Process.*, **1** (2019), 44–62. https://doi.org/10.1016/j.sigpro.2018.09.029
45. A. Rehman, X. Liao, R. Ashraf, S. Ullah, H. Wang, A color image encryption technique using exclusive-OR with DNA complementary rules based on chaos theory and SHA-2, *Optik*, **1** (2019), 348–367. https://doi.org/10.1016/j.ijleo.2018.01.064
46. D. Shah, T. Shah, S. S. Jamal, A novel efficient image encryption algorithm based on affine transformation combined with linear fractional transformation, *Multidimensional Syst. Signal Process.*, **1** (2015), 885–905. https://doi.org/10.1007/s11042-020-09892-5
47. J. Wu, X. Liao, B. Yang, Color image encryption based on chaotic systems and elliptic curve ElGamal scheme, *Signal Process.*, **141** (2017), 109–124. https://doi.org/10.1016/j.sigpro.2017.04.006
48. A. U. Rehman, J. S. Khan, J. Ahmad, S. O. Hwang, A new image encryption scheme based on dynamic S-boxes and chaotic maps, *3D Res.*, **7** (2016), 7. https://doi.org/10.1007/s13319-016-0084-9
49. I. Khalid, S. S. Jamal, T. Shah, D. Shah, M. M. Hazzazi, A novel scheme of image encryption based on elliptic curves isomorphism and substitution boxes, *IEEE Access*, **9** (2021), 77798–77810. https://doi.org.10.1109/ACCESS.2021.3083151